PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-189526

(43)Date of publication of application : 05.07.2002

---

(51)Int.Cl. G06F 1/00

G06F 13/00

G06F 17/60

H04L 9/08

---

(21)Application number : 2000-389679 (71)Applicant : NEC CORP

(22)Date of filing : 22.12.2000 (72)Inventor : NAKAMURA NOBUTATSU

---

(54) DISTRIBUTION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the distribution system of software with use constraint for easily preparing and distributing data and software with use constraint to a user, and for allowing the user to easily use the data and software.

SOLUTION: A distribution server 1 enciphers data and software with use constraint and a use condition by an encipherment processing part 11 by using a cryptographic key corresponding to a terminal client 2 at the destination of distribution, and packages them by a package part 15, and transmits them through a communicating part 10. The terminal client 2 decodes the use condition by using a cryptographic key by an encipherment processing part 21, and when the use condition is available, decodes and installs the data and software. Also, when starting another program, the decoded data and software are uninstalled, and the updated use condition or data and software are enciphered and stored.

LEGAL STATUS [Date of request for examination] 12.08.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The distribution server which package-izes [code-] delivery information which consists of either [at least] data with utilization constraint, or software, and distributes it, It is the distribution system which consists of a terminal client using said distributed data with utilization constraint or software. Said distribution server The 1st management tool which manages and sets up the utilization conditions of delivery information which consist of either [at least] said data with utilization constraint, or software, An encryption means to encipher said delivery information and said utilization conditions using the cryptographic key corresponding to said terminal client of a distribution place, The activation code of the program corresponding to said terminal client of said distribution place, and the 2nd management tool which manages and sets up said enciphered install information on delivery information, It has a package means to package-ize said enciphered delivery information, said utilization conditions, and

said install information to the program of one execute form. Said terminal client A storage means by which memorize at least the package distributed from said server, and the updating storage of said utilization conditions in this package is enciphered and carried out after that, Said utilization conditions enciphered from the information read from said storage means are extracted. A judgment means to decode using the cryptographic key assigned beforehand and to judge authorization and the disapproval of utilization according to the decoded utilization condition, When said package memorized by said storage means is a package with which utilization was permitted by said judgment means The distribution system characterized by having a decode means to decode said enciphered delivery information in the package, and the means which changes processing control to access and the program to be used after performing install processing of said software from said decode means.

[Claim 2] Said terminal client is a distribution system according to claim 1 characterized by having a means to uninstall said delivery information decoded by said decode means when utilization of said delivery information is judged by said judgment means to be disapproval, or when the program of other arbitration is started.

[Claim 3] Said 1st management tool of said distribution server sets up the count of available as said utilization conditions. Said judgment means of said terminal

client While recording the count of a utilization track record at every utilization of said data or software The distribution system according to claim 1 characterized by judging the propriety of utilization of said delivery information by computing the count of residual available from the count of a utilization track record, and said count of available decoded from said package.

[Claim 4] Said 1st management tool of said distribution server sets up the count of available as said utilization conditions. Said judgment means of said terminal client While supervising program execution, counting the count of generating of a specific program event as said data or a count of utilization of software and recording it during utilization of the distributed said data or software By computing the count of residual available to the utilization time of said distributed data or software from said count of utilization, and said count of available decoded from said package The distribution system according to claim 1 characterized by judging the propriety of utilization of said distributed data or software.

[Claim 5] It is the distribution system according to claim 1 which said 1st management tool of said distribution server sets up an available period as said utilization conditions, and is characterized by judging the propriety of utilization of said delivery information because said judgment means of said terminal client compares current time with said available period decoded from said package at

every utilization of said delivery information.

[Claim 6] It is the distribution system according to claim 1 which said 1st management tool of said distribution server sets up available time as said utilization conditions, and said judgment means of said terminal client adds the utilization track record time amount of the delivery information during utilization of said delivery information, computes residual available time from the utilization track record time amount and said available time decoded from said package, and is characterized by to judge the propriety of utilization of said delivery information according to this computed residual available time.

[Claim 7] Said 1st management tool of said distribution server sets up available time as said utilization conditions. Said terminal client A timer setting-out means for residual available time to be set up as a timer value, and to set up the alarm timer for stopping utilization of said delivery information under utilization if the timer value passes, It has a means to update and encipher and to record said residual available time while canceling said alarm timer set up by said timer setting-out means at the time of utilization termination of said delivery information. The distribution system according to claim 1 characterized by decoding said residual available time currently enciphered and recorded, and making it set up as a timer value with said timer setting-out means whenever it decodes said delivery information with said decode means.

[Claim 8] It is the distribution system according to claim 1 which said 1st management tool of said distribution server sets up prohibition of utilization of the delivery information copied as said utilization conditions, and is characterized by for said judgment means of said terminal client responding for whether being the information to which said delivery information was copied, and judging the propriety of utilization of said delivery information.

[Claim 9] At the times other than the utilization time of said delivery information, said terminal client this delivery information It enciphers with said utilization conditions and has the updating means which carries out updating storage as said package for said storage means. Said judgment means The distribution system according to claim 8 characterized by judging whether it is the information to which said delivery information was copied by comparing the modification time of said delivery information by which was enciphered by said updating means and updating storage was carried out with the modification time which a file system manages.

[Claim 10] It is the distribution system according to claim 1 which said 1st management tool of said distribution server sets up the utilization C only in a specific terminal client as said utilization conditions, and is characterized by said encryption means enciphering delivery information using the cryptographic key which enables decode of delivery information only by the specific terminal client.

[Claim 11] Only the user of the specification [said 1st management tool of said distribution server] as said utilization conditions is the distribution system according to claim 1 which it sets up that utilization is possible, and said encryption means enciphers data using the cryptographic key which makes decode possible for data only with the specific user's password, and is characterized by equipping said terminal client with a means to acquire said specific user's password.

[Claim 12] A monitor means by which said terminal client supervises starting of the program of arbitration, A detection means to detect whether said delivery information is using when said monitor means detects starting of other programs of said arbitration, When it is detected that said delivery information is using with said detection means The distribution system according to claim 1 characterized by having a means to encipher the delivery information which decodes under utilization, and the updated utilization conditions, and to memorize as said package for said storage means, and a means to uninstall the delivery information which decodes under said utilization.

[Claim 13] It is [claim 1 characterized by having equipped said distribution server with the 1st means of communications which communicates with said terminal client further, and equipping said terminal client with the 2nd means of communications which communicates with said distribution server further

thru/or] a distribution system given in any 1 term among 12.

[Claim 14] Said terminal client is a distribution system according to claim 13 which acquires said execution information from said distribution server at the time of a transmitting means to transmit execution information to said distribution server at the time of utilization initiation of said delivery information, and utilization termination of said delivery information, and carries out the description of having had a means to eliminate the delivery information in the condition of having decoded, from a storage region.

[Claim 15] It is the distribution system according to claim 13 or 14 which said 1st management tool of said distribution server sets up that utilization is possible only from a specific network as said utilization conditions, and said encryption means enciphers this delivery information using the cryptographic key which enables decode of said delivery information only at the network address of said specific terminal client, and is characterized by equipping said terminal client with a means to acquire said network address.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to a distribution system, especially relates to the distribution system which distributes the data and software which set up utilization conditions and are distributed to a user.

[0002]

[Description of the Prior Art] Generally the count of utilization, the utilization time, utilization length, and the prohibition on a copy being set up according to the sample offer object or the purchase amount of money, and distributing data and software is performed, and an example of the distribution system is proposed in JP,7-325713,A (the name of invention: the software activation approach with constraint of the utilization time).

[0003] As shown in drawing 10 , this conventional distribution system consists of the offer software 901, the key information preservation section 902, an executive supervisor 903, and install/copying program 904, enciphers the individual identification information of the hardware in which the available time of the offer software 901, the time of a due date, and the offer software 901 are installed first, and the physical location information on a storage region that the offer software 901 is memorized, and carries out storage maintenance at the key information preservation section 902.

[0004] With reference to the information currently enciphered and held at the key

information preservation section 902, an executive supervisor 903 checks the justification of activation of software, and supervises available time during activation of the offer software 901, and when time amount is exceeded, it terminates activation of the offer software 901. Install / copying program 904 is used, in case the offer software 901 is installed in a computer or it is copied to an alien machine.

[0005] Conventionally [this], in a system, since the enciphered key information cannot be decoded correctly and offer software 901 cannot be performed even if it installs and copies the offer software 901, without using install / copying program 904, unrestricted utilization and an unrestricted copy of the offer software 901 can be restricted.

[0006] Moreover, a distribution means to read so that read-out may be impossible to onerous information, an install program, and utilization information as other conventional distribution systems, and to restrict, and to distribute to a user system from a provider system, with a limit discharge means to carry out reading appearance to the onerous information, the above-mentioned install program, and above-mentioned utilization information which were distributed, and to cancel a limit while starting the install program of which reading appearance was carried out and the limit was canceled, only when a judgment means to judge the propriety of utilization of onerous information based on the

utilization information of which reading appearance was carried out and the limit was canceled, and a judgment means judge affirmation An install means to read the onerous information of which the read-out limit was canceled, and to perform processing required for install of onerous information based on an install program, When install by the install means is completed The distribution system equipped with the limit means which reads to the onerous information in the condition that the read-out limit was canceled, restricts, and is written in a storage means is also known (JP,2000-200229,A: name of invention "an onerous information distribution system and the onerous information distribution approach".).

[0007]

[Problem(s) to be Solved by the Invention] However, I hear that the provider of software needs modification of a program to the offer software 901, and needs install / copying program 904 of dedication in the case of user distribution, and the 1st trouble of the conventional system given [above-mentioned] in JP,7-325713,A has him.

[0008] The reason will be because it is necessary to add a program which stops the offer software 901, if there is no right utilization condition information. Moreover, if install / copying program 904 of dedication are not used, it is because said utilization condition information is not installed correctly.

[0009] It is not enciphered, but since the modification is easy, I hear that illegal utilization and an illegal copy of the offer software 901 are easy for the offer software 901, and the 2nd trouble has it.

[0010] moreover, after distributing various information with utilization constraint to a user system and being complete install in the user system of a distribution place, he restrict by carrying out reading appearance to onerous information, and he be trying to write in a storage means in the conventional system given [above-mentioned] in JP,2000-200229,A, but since it be restricting by an install program carrying out reading appearance, there be a problem that where of the analysis of an install program will be attain by other programs. Moreover, since utilization conditions are not manageable by the provider system side, modification of utilization conditions is not easy.

[0011] It aims at offering the distribution system of the software with utilization constraint with which this invention was made in view of the above point, creates data and software with utilization constraint easily, and distributes them to a user, and a user can use the data and software easily.

[0012] Moreover, other objects of this invention are to offer the distribution system of the software with utilization constraint which makes difficult data with utilization constraint, and illegal utilization and an illegal copy of software.

[0013]

[Means for Solving the Problem] The distribution server which package-izes [code-] delivery information which consists of either [at least] data with utilization constraint, or software, and distributes it in order that this invention may attain the above-mentioned object, It is the distribution system which consists of a terminal client using the distributed data with utilization constraint or software. A distribution server The 1st management tool which manages and sets up the utilization conditions of delivery information which consist of either [at least] data with utilization constraint, or software, An encryption means to encipher delivery information and utilization conditions using the cryptographic key corresponding to the terminal client of a distribution place, The 2nd management tool which manages and sets up the install information on the delivery information enciphered as the activation code of the program corresponding to the terminal client of a distribution place, It has a package means to package-ize the enciphered delivery information, utilization conditions, and install information to the program of one execute form. A terminal client A storage means by which memorize at least the package distributed from the server, and the updating storage of the utilization conditions in a package is enciphered and carried out after that, The utilization conditions enciphered from the information read from the storage means are extracted. A judgment means to decode using the cryptographic key assigned beforehand and to judge

authorization and the disapproval of utilization according to the decoded utilization condition, When the package memorized by the storage means is a package with which utilization was permitted by the judgment means It considers as the configuration equipped with a decode means to decode the delivery information as which it was enciphered in the package, and the means which changes processing control to access and the program to be used after performing install processing of the software from a decode means.

[0014] In this invention, without recompiling delivery information, such as data with utilization constraint, and software with utilization constraint, it can encipher, after adding utilization conditions, and it can distribute to a terminal client, and delivery information can be decoded and used according to utilization conditions.

[0015] Moreover, in order to attain the above-mentioned object, this invention is characterized by having a means to uninstall the delivery information decoded by the decode means, when utilization of delivery information is judged by the judgment means in the above-mentioned terminal client to be disapproval, or when the program of other arbitration is started.

[0016] In this invention, when the program of other arbitration is started, the delivery information decoded by the decode means can be uninstalled. Moreover, by this invention, it can save in the condition of having been enciphered, in a terminal client except the utilization time of delivery information.

[0017] Moreover, in order to attain the above-mentioned object, it is characterized by having a means by which this invention eliminates the delivery information in the condition that the terminal client acquired execution information from the distribution server at the time of a transmitting means to transmit execution information to a distribution server at the time of utilization initiation of delivery information, and utilization termination of delivery information, and was decoded, from a storage region. Since execution information, such as utilization conditions, is transmitted to the distribution server at the time of utilization initiation of delivery information, the utilization conditions of a terminal client etc. are manageable by the distribution server side with this invention.

[0018]

[Embodiment of the Invention] Next, the gestalt of operation of this invention is explained with a drawing. Drawing 1 shows the block diagram of the gestalt of operation of the 1st of the distribution system which becomes this invention. As shown in this drawing, the gestalt of operation of the 1st of this invention consists of terminal clients 2 using the distribution server 1 which package-izes [code-] offer data and software with utilization constraint, and distributes them, and the data and software which were distributed.

[0019] The communications department 10 where the distribution server 1

communicates with the terminal client 2, and the cipher-processing section 11 which enciphers offer data and software, With the cryptographic key Management Department 12 holding the cryptographic key used in case the cipher-processing section 11 carries out cipher processing With the starting Research and Data Processing Department 13 which manages the starting information for performing the data distributed to the terminal client 2 With the utilization condition Research and Data Processing Department 14 holding offer data and the utilization conditions of software The package section 15 which package-izes the offer data and software which were enciphered as aforementioned starting information and aforementioned utilization conditions, and the offer software attaching part 16 holding offer data and the former data of software are included.

[0020] The communications department 20 where the terminal client 2 communicates with the distribution server 1, and the cipher-processing section 21 which enciphers the data on a decryption and a storage region for the distributed data, With the cryptographic key Management Department 22 holding the cryptographic key used in case the cipher-processing section 21 carries out cipher processing The activation Monitoring Department 23 which supervises a program execution situation and performs interruption processing to a certain activation situation, the execution information Management

Department 24 which manages the various information used at the activation Monitoring Department 23, and the software activation section 25 which carries out executive operation of the program are included.

[0021] Next, with reference to the flow chart of drawing 2 , actuation of the distribution server 1 of the gestalt of operation of the 1st of drawing 1 is explained to a detail. First, starting of the distribution server 1 waits for the distribution demand from the terminal client 2 in the communications department 10 (step 101). If there is a distribution demand, the cipher-processing section 11 will acquire the offer data and software which were demanded from the offer software attaching part 16 (step 102), and will choose the encryption algorithm used for encryption of the offer data and software (step 103).

[0022] Next, the cipher-processing section 11 identifies the terminal client 2 of distribution demand origin based on the discernment ID of terminal client 2 proper contained in the distribution demand, from the cryptographic key Management Department 12, the cryptographic key corresponding to the terminal client 2 of the distribution place memorized beforehand is extracted (step 104), and offer data and software are enciphered using the cryptographic key and cryptographic algorithm which were extracted (step 105).

[0023] Next, the package section 15 extracts the data with utilization constraint distributed to the terminal client 2, and the starting information on software

(namely, offer data and software) from the starting Research and Data Processing Department 13 (step 106). The install code which installs the program activation code corresponding to the terminal client 2, offer data, and software in the storage region of the terminal client 2, and the program termination code set up so that control might move to offer software automatically are included in starting information. The above-mentioned program termination code will turn into a program termination code set up so that control might move to the access software corresponding to the format of the data automatically, if offer software is image data and text data.

[0024] Next, the package section 15 extracts the offer data in the terminal client 2, and the utilization condition information on software from the utilization condition Research and Data Processing Department 14 (step 107). Either of the parameters about the cryptographic algorithm used for encryption of the count of utilization, the utilization time, a utilization period, the propriety of copy utilization, a utilization location, a user, a utilization terminal, and offer software is contained in utilization condition information. Furthermore, the extracted utilization condition information is enciphered by the cipher-processing section 11 (step 108).

[0025] Next, the package section 15 package-izes the offer data enciphered at step 105 and software, starting information generated at step 106, and utilization

condition information enciphered at step 108 (step 109). The package-ized data serve as a distribution activation package of the format which can be performed by the terminal client 2 as it is. The utilization condition information and offer software which were enciphered are set up so that it may be treated as a program resource of a distribution activation package.

[0026] Then, if it confirms whether the error occurred, for example in a series of processings of step 101 of the above [the package section 15] thru/or step 109 (step 110) and is errorless, the communications department 10 will distribute the distribution activation package from the package section 15 to the terminal client 2 (step 111), and if there is an error, error information will be notified to the terminal client 2 (step 112).

[0027] Next, with reference to the flow chart of drawing 3 and drawing 4 , the actuation when starting the distribution activation package in the terminal client 2 of the gestalt of operation of the 1st of drawing 1 is explained to a detail.

[0028] First, in the communications department 20, the terminal client 2 acquires the distribution activation package distributed from the distribution server 1, and saves it in the storage region. The software activation section 25 starts the distribution activation package saved in the above-mentioned storage region with directions of a user (step 201). The activation Monitoring Department 23 is supervising starting of the program of arbitration, and if the started program

judges whether it is a distribution activation package and it is a distribution activation package, it will wedge for it itself and process processing of the flow chart shown in drawing 4 (step 202).

[0029] In interruption processing, the activation Monitoring Department 23 notifies and records the identification information of the distribution activation package of an interrupting agency on the execution information Management Department 24 first (step 211). Furthermore, the cipher-processing section 21 extracts a cryptographic key from the cryptographic key Management Department 22 (step 212). If the cryptographic key Management Department 22 is required, it will acquire a user's password, the proper identification information of a terminal, the network address information on a terminal, and geographical positional information, and will generate a cryptographic key.

[0030] Then, it is confirmed whether using the extracted cryptographic key, the cipher-processing section 21 decodes utilization condition information first (step 213), and has utilization authorization of offer data and software with reference to the decoded utilization condition further (step 214). The check referred to as whether to be data with which it was copied whether the count of a utilization track record has exceeded the count of available, whether utilization track record time amount has exceeded available time (is the count of residual utilization larger than zero or not?), and whether time has passed over utilization length (is

the residual utilization time larger than zero or not?) will be performed if required. It is possible to judge it as the data manipulation time included in utilization conditions by whether the data manipulation time according [whether it is copied data] to the file system of the terminal client 2 is in agreement.

[0031] In step 214, when it is judged that there is utilization authorization of offer data and software, the cipher-processing section 21 performs decode processing of offer data and software (step 215). On the other hand, in step 214, if the case where it is judged that there is no utilization authorization of offer data and software, and decode processing have an error, that will be notified and recorded on the execution information Management Department 24 (step 216). And control is returned to the distribution activation package of an interrupting agency.

[0032] After interruption processing termination, although the execution information Management Department 24 is notified of the error, if it confirms how it is (step 203) and there is an error, a user will be notified of the content of the error (step 205). For example, it displays by the display which does not illustrate the message of that utilization length passed, data being altered for the copy etc. which the count of utilization became more than the count of a convention, and which the utilization time became beyond convention time amount. An error of the execution information Management Department 24 is cleared after a display.

[0033] In step 203, when judged with the execution information Management Department 24 not being notified of the error, the offer data and software which were decoded are recorded on a suitable storage region, and install processing is performed (step 204). Next, if required, an alarm timer will be registered in order to set up a utilization time limit (step 206). At this time, with reference to utilization conditions, the timer value of the alarm timer registered extracts the remaining available time, and is set as that remaining available time.

[0034] If it passes over the time amount of this timer value, it will set up so that alarm interruption starting of the distribution activation package may be carried out and activation may be suspended. Furthermore, processing of a distribution activation package is ended, access / utilization software or offer software of offer data is started, and processing control is moved (step 207).

[0035] Next, with reference to each flow chart of drawing 5 and drawing 6 , the terminal client 2 of the gestalt of operation of the 1st of drawing 1 explains the actuation when starting the program of arbitration to a detail.

[0036] The terminal client 2 starts the program of arbitration in the software activation section 25 (step 301). The activation Monitoring Department 23 is supervising starting of the program of arbitration, and if the started program judges whether it is the offer software of a distribution activation package and it is not offer software, it will wedge for it itself and process processing of the flow

chart shown in drawing 6 (step 302).

[0037] In interruption processing, the identification information of a distribution activation package is first extracted from the execution information Management Department 24 (step 311). The identification information of this distribution activation package returns control to the program of an interrupting agency, if it is recorded at said step 211 and identification information does not exist. The following processings are performed, in order to call it under utilization of offer data and software and to prevent other copies and alterations according offer data and software to a program, if identification information exists.

[0038] Moreover, since it is going to use offer data and software when in agreement with the identification information of the program of an interrupting agency, control is returned to the program of an interrupting agency. It will be made to end if offer data and software are using.

[0039] The execution information Management Department 24 updates the utilization condition information about utilization hysteresis which offer data and software used, such as a count and time amount, (step 312). Next, like step 212, from the cryptographic key Management Department 22, the cipher-processing section 21 extracts a cryptographic key (step 313), and enciphers utilization condition information using the extracted cryptographic key (step 314). Furthermore, the offer data and software which are decoded by the storage

region of the terminal client 2 from a distribution activation package, and are installed in it are enciphered including running state information (step 315). As long as running state information does not exist or offer data and software do not need to save, processing of step 315 may be omitted.

[0040] Next, the enciphered utilization condition information, the enciphered offer data, and software are stored in a distribution activation package (step 316). Furthermore, the offer data and software which are installed in the terminal client 2 are uninstalled, and are deleted from the storage region of the terminal client 2 (step 317). A memory area will also be cleared if required.

[0041] In said step 206, if the alarm timer is set up, this will be canceled (step 318). And control is returned to the program of an interrupting agency. After interruption processing termination usually processes (step 303).

[0042] thus, when the program of arbitration is started Supervise whether the identification information of a distribution activation package exists, and if it does not exist, since it is not starting of offer data and software but starting of other programs Since he is trying to delete the data with utilization constraint and software which were being used till then by interruption processing from the storage region of the terminal client 2, Data with utilization constraint and software can be copied by other programs, or can prevent being altered. However, it enciphers and data with utilization constraint and software are again

stored in the package.

[0043] Next, with reference to each flow chart of drawing 7 and drawing 8 , the terminal client 2 of the gestalt of operation of the 1st of drawing 1 explains actuation while using offer data and software to a detail.

[0044] First, if alarm advice is given by the alarm timer set up in said step 206 (step 401), by zero, the residual utilization time will end utilization of offer data and software (step 402), and will perform processing of step 312 thru/or step 318 shown in the flow chart of drawing 6 (step 403). Thereby, a user cannot use offer data and software any more.

[0045] Moreover, the activation Monitoring Department 23 is supervising the event processing specified during offer software activation, and if the specified event processing occurs (step 501), it will perform interruption processing after step 502 of drawing 8 . The specified event processing is things, such as drawing of a window, and a user's mouse click.

[0046] In interruption processing, it investigates whether it is in agreement with the event registered into the utilization condition information that the event is held at the execution information Management Department 24 (step 502). If not in agreement, it usually returns to processing (step 507). If in agreement, after updating the utilization condition information about utilization hysteresis (step 503), with reference to utilization conditions, it will be confirmed whether offer

data and software are still available (step 504).

[0047] If still available, it will usually return to processing (step 507). If utilization is improper, utilization of offer data and software will be ended (step 505), and uninstallation processing of step 312 thru/or step 318 shown in the flow chart of drawing 6 will be performed (step 506).

[0048] Next, the effectiveness of the gestalt of this operation is explained. Since it consists of gestalten of this operation, without recompiling offer data and software so that addition and encryption may be given and utilization conditions may be distributed in the terminal client 2 in the format which can be performed, data and software with utilization constraint can be created easily, and a user can be supplied widely, and a user can use data and software with utilization constraint easily.

[0049] Moreover, further, in the terminal client 2, except utilization time, since offer data and software are constituted so that it may be saved in the condition of having been enciphered, with the gestalt of this operation, they can make difficult illegal utilization and an illegal copy of software with utilization constraint.

[0050] Next, the gestalt of operation of the 2nd of this invention is explained to a detail with reference to a drawing. Drawing 9 shows the block diagram of the gestalt of operation of the 2nd of the distribution system which becomes this invention. The same sign is given to the same component as drawing 1 among

this drawing, and the explanation is omitted. As shown in drawing 9 , the gestalt of operation of the 2nd of this invention has the description in the point which has the composition of having excluded the execution information Management Department 24 where the terminal client 3 is contained in the terminal client 2 in the gestalt of operation of the 1st of drawing 1 .

[0051] With the gestalt of this operation, through the communications department 20, the terminal client 3 transmits data to a distribution server side, and performs the information management function equivalent to said execution information Management Department 24 in the utilization condition Research and Data Processing Department 14 of the distribution server 1. If required, in order to prevent unjust acquisition of the data at the time of a communication link, it is possible to use the cipher-processing section 11 of the distribution server 1 and the cipher-processing section 21 of the terminal client 3, to encipher data and to communicate. Since the detail of an encryption communication link is known more generally than before, the explanation by this invention is omitted.

[0052] Next, the effectiveness of the gestalt of this operation is explained. Since it consists of gestalten of this operation so that utilization condition information and a utilization situation may be managed by the distribution server 1 side, unjust updating and an unjust alteration of utilization conditions can be made more difficult.

[0053] Moreover, offer data and the utilization conditions of software can be changed, without updating the software currently held at a user's terminal client 3, even when utilization conditions are updated by that a user pays offer data and the utilization tariff of software etc.

[0054] In addition, although this invention is not limited to the gestalt of the above operation, and it is constituted so that the distribution server 1 and the terminal client 2 may exchange data through communication networks, such as the Internet, with the gestalt of the 1st and the 2nd operation for example, of course, this invention is applicable also to the system which exchanges data through record media, such as a floppy (trademark) disk and CD-ROM.

[0055] Moreover, even when exchanging data through a communication network, the distribution server 1 sets up that utilization is possible only from a specific network as utilization conditions, it considers as the configuration enciphered using the cryptographic key to which the cipher-processing section 11 enables decode of data with utilization constraint, and software only at the network address of a specific terminal client, and the terminal client 2 or 3 is good also as a configuration which acquires a network address. Furthermore, one distribution of not only distribution of both data with utilization constraint and software but data with utilization constraint and software with utilization constraint is sufficient.

[0056]

[Effect of the Invention] Since encipher after adding utilization conditions, and it distributes to a terminal client, delivery information is decoded according to utilization conditions and it made use according to this invention as explained above, without recompiling delivery information, such as data with utilization constraint, and software with utilization constraint, the distribution system by which data and software with utilization constraint are easily created, and a user is supplied widely, and a user can perform the software easily can build.

[0057] Moreover, since according to this invention the delivery information decoded by the decode means was uninstalled when the program of other arbitration was started, analysis, an alteration, etc. of the alteration of the data of delivery information or software which were decoded by other programs can be prevented.

[0058] Moreover, according to this invention, in a terminal client, except the utilization time of delivery information, since delivery information was saved in the condition of having been enciphered, illegal utilization and an illegal copy of delivery information can be made difficult.

[0059] Moreover, since the utilization conditions of a terminal client etc. were managed by the distribution server side by transmitting execution information, such as utilization conditions, to a distribution server at the time of utilization initiation of delivery information according to this invention, modification of

utilization conditions can be performed easily.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the configuration of the 1st of the gestalt of operation of this invention.

[Drawing 2] It is the flow chart which shows actuation of the distribution server of the gestalt of the 1st operation.

[Drawing 3] It is the flow chart which shows the offer data of the terminal client of the gestalt of the 1st operation, and software utilization time processing actuation.

[Drawing 4] It is the flow chart which shows interruption processing actuation of the offer data of the terminal client of the gestalt of the 1st operation, and software utilization time.

[Drawing 5] It is the flow chart which shows software execution-time processing actuation of the arbitration of the terminal client of the gestalt of the 1st operation.

[Drawing 6] It is the flow chart which shows the interruption processing actuation

at the time of software activation of the arbitration of the terminal client of the gestalt of the 1st operation.

[Drawing 7] It is the flow chart which shows the alarm processing actuation under offer software utilization of the terminal client of the gestalt of the 1st operation.

[Drawing 8] It is the flow chart which shows the event interruption processing actuation under offer software utilization of the terminal client of the gestalt of the 1st operation.

[Drawing 9] It is the block diagram showing the configuration of the 2nd of the gestalt of operation of this invention.

[Drawing 10] It is the block diagram of a conventional example.

[Description of Notations]

1 Distribution Server

2 Three Terminal client

10 20 Communications department

11 21 Cipher-processing section

12 22 Cryptographic key Management Department

13 Starting Research and Data Processing Department

14 Utilization Condition Research and Data Processing Department

15 Package Section

16 Offer Software Attaching Part

23 Activation Monitoring Department

24 Execution Information Management Department

25 Software Activation Section

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－189526
（P2002－189526A）
(43)公開日　平成14年７月５日(2002.7.5)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
G06F	1/00		G06F	13/00	540S　5B076
	13/00	540		17/60	124　5J104
	17/60	124			142
		142		9/06	660F
H04L	9/08		H04L	9/00	601D

審査請求　未請求　請求項の数15　ＯＬ　（全 10 頁）

(21)出願番号　特願2000－389679(P2000－389679)

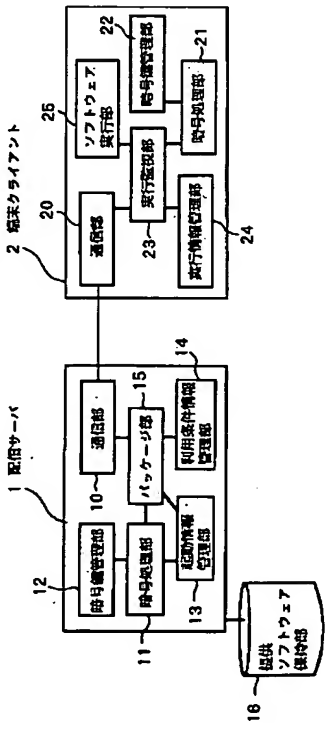
(22)出願日　平成12年12月22日(2000.12.22)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　中村　暢達
東京都港区芝５丁目７番１号　日本電気株式会社内
(74)代理人　100085235
弁理士　松浦　兼行

Ｆターム(参考)　5B076 FA01 FB01 FB06 FB17 FB18
5J104 AA01 AA16 EA02 EA04 EA26
NA02 NA05 PA07

(54)【発明の名称】　配信システム

(57)【要約】
【課題】　従来は、ソフトウェアの提供者は利用者配布の際には専用のインストール／複写プログラムを必要とし、また、提供ソフトウェアが暗号化されておらず、違法な利用や複写が容易である。
【解決手段】　配信サーバ１は、利用制約付きデータ及びソフトウェアと利用条件を、配信先の端末クライアント２に対応する暗号鍵を用いて暗号処理部１１で暗号化し、更にパッケージ部１５でパッケージ化した後、通信部１０を介して送信する。端末クライアント２は、暗号処理部２１で暗号鍵を用いて利用条件を復号し、その利用条件が利用可であるときには、データ及びソフトウェアを復号してインストールする。また、他のプログラムの起動時は復号したデータ及びソフトウェアはアンインストールすると共に、更新後の利用条件やデータ及びソフトウェアを暗号化して記憶する。



【特許請求の範囲】

【請求項１】　利用制約付きデータ及びソフトウェアの少なくとも一方からなる配信情報を暗号パッケージ化して配信する配信サーバと、配信された前記利用制約付きデータ又はソフトウェアを利用する端末クライアントからなる配信システムであって、

前記配信サーバは、

前記利用制約付きデータ及びソフトウェアの少なくとも一方からなる配信情報の利用条件を管理及び設定する第１の管理手段と、

前記配信情報と前記利用条件を、配信先の前記端末クライアントに対応する暗号鍵を用いて暗号化する暗号化手段と、

前記配信先の前記端末クライアントに対応したプログラムの起動コードと前記暗号化された配信情報のインストール情報を管理及び設定する第２の管理手段と、

前記暗号化された配信情報と、前記利用条件と、前記インストール情報とを１つの実行形式のプログラムにパッケージ化するパッケージ手段とを備え、前記端末クライアントは、

前記サーバから配信されたパッケージを少なくとも記憶し、その後に該パッケージ中の前記利用条件が暗号化されて更新記憶される記憶手段と、

前記記憶手段から読み出した情報から暗号化された前記利用条件を抽出して、予め割り当てられた暗号鍵を用いて復号し、その復号した利用条件に応じて利用の許可・不許可を判定する判定手段と、

前記記憶手段に記憶された前記パッケージが前記判定手段により利用の許可されたパッケージである時には、そのパッケージ中の前記暗号化された配信情報を復号する復号手段と、

前記復号手段からの前記ソフトウェアのインストール処理を行ってから閲覧・利用するプログラムに処理制御を切り替える手段とを備えたことを特徴とする配信システム。

【請求項２】　前記端末クライアントは、前記判定手段により前記配信情報の利用が不許可と判定されたとき、又は他の任意のプログラムが起動されたときには、前記復号手段により復号された前記配信情報をアンインストールする手段を有することを特徴とする請求項１記載の配信システム。

【請求項３】　前記配信サーバの前記第１の管理手段は、前記利用条件として利用可能回数を設定し、前記端末クライアントの前記判定手段は、前記データ又はソフトウェアの利用の都度、利用実績回数を記録すると共に、その利用実績回数と前記パッケージから復号した前記利用可能回数とから残存利用可能回数を算出することで、前記配信情報の利用の可否を判断することを特徴とする請求項１記載の配信システム。

【請求項４】　前記配信サーバの前記第１の管理手段は、前記利用条件として利用可能回数を設定し、前記端末クライアントの前記判定手段は、配信された前記データ又はソフトウェアの利用中に、プログラムの実行を監視し、特定のプログラムイベントの発生回数を前記データ又はソフトウェアの利用回数としてカウントして記録すると共に、配信された前記データ又はソフトウェアの利用時に前記利用回数と前記パッケージから復号した前記利用可能回数とから残存利用可能回数を算出することで、配信された前記データ又はソフトウェアの利用の可否を判定することを特徴とする請求項１記載の配信システム。

【請求項５】　前記配信サーバの前記第１の管理手段は、前記利用条件として利用可能期間を設定し、前記端末クライアントの前記判定手段は、前記配信情報の利用の都度、現在時刻と前記パッケージから復号した前記利用可能期間を比較することで前記配信情報の利用の可否を判定することを特徴とする請求項１記載の配信システム。

【請求項６】　前記配信サーバの前記第１の管理手段は、前記利用条件として利用可能時間を設定し、前記端末クライアントの前記判定手段は、前記配信情報の利用中にその配信情報の利用実績時間を加算し、その利用実績時間と前記パッケージから復号した前記利用可能時間とから残存利用可能時間を算出し、算出した該残存利用可能時間に応じて前記配信情報の利用の可否を判定することを特徴とする請求項１記載の配信システム。

【請求項７】　前記配信サーバの前記第１の管理手段は、前記利用条件として利用可能時間を設定し、前記端末クライアントは、残存利用可能時間がタイマ値として設定され、そのタイマ値が経過すると利用中の前記配信情報の利用を停止させるためのアラームタイマを設定するタイマ設定手段と、前記配信情報の利用終了時に前記タイマ設定手段により設定された前記アラームタイマを解除すると共に前記残存利用可能時間を更新及び暗号化して記録する手段とを有し、前記復号手段により前記配信情報を復号する都度、暗号化して記録されている前記残存利用可能時間を復号して前記タイマ設定手段によりタイマ値として設定させることを特徴とする請求項１記載の配信システム。

【請求項８】　前記配信サーバの前記第１の管理手段は、前記利用条件として複写された配信情報の利用禁止を設定し、前記端末クライアントの前記判定手段は、前記配信情報が複写された情報かどうかに応じて前記配信情報の利用の可否を判定することを特徴とする請求項１記載の配信システム。

【請求項９】　前記端末クライアントは、前記配信情報の利用時以外の時には該配信情報を、前記利用条件と共に暗号化して前記記憶手段に前記パッケージとして更新記憶しておく更新手段を有し、前記判定手段は、前記更新手段により暗号化されて更新記憶された前記配信情報

の更新時刻と、ファイルシステムが管理する更新時刻とを比較することで、前記配信情報が複写された情報であるかどうかを判定することを特徴とする請求項８記載の配信システム。

【請求項１０】　前記配信サーバの前記第１の管理手段は、前記利用条件として特定の端末クライアントのみでの利用可を設定し、前記暗号化手段は、その特定の端末クライアントでのみ配信情報の復号を可能とする暗号鍵を用いて配信情報を暗号化することを特徴とする請求項１記載の配信システム。

【請求項１１】　前記配信サーバの前記第１の管理手段は、前記利用条件として特定の利用者のみ利用可と設定し、前記暗号化手段は、その特定の利用者のパスワードでのみデータを復号を可能とする暗号鍵を用いてデータを暗号化し、前記端末クライアントは、前記特定の利用者のパスワードを取得する手段を備えたことを特徴とする請求項１記載の配信システム。

【請求項１２】　前記端末クライアントは、任意のプログラムの起動を監視する監視手段と、前記監視手段により前記任意の他のプログラムの起動を検出した時に前記配信情報が利用中であるかどうか検出する検出手段と、前記検出手段により前記配信情報が利用中であると検出された時には、利用中の復号されている配信情報と更新した利用条件を暗号化して前記記憶手段に前記パッケージとして記憶する手段と、前記利用中の復号されている配信情報をアンインストールする手段とを備えたことを特徴とする請求項１記載の配信システム。

【請求項１３】　前記配信サーバは、前記端末クライアントと通信する第１の通信手段をさらに備え、前記端末クライアントは、前記配信サーバと通信する第２の通信手段をさらに備えたことを特徴とする請求項１乃至１２のうちいずれか一項記載の配信システム。

【請求項１４】　前記端末クライアントは、前記配信情報の利用開始時に実行情報を前記配信サーバに送信する送信手段と、前記配信情報の利用終了時に前記実行情報を前記配信サーバより取得して、復号された状態の配信情報を記憶領域より消去する手段を備えたことを特徴する請求項１３記載の配信システム。

【請求項１５】　前記配信サーバの前記第１の管理手段は、前記利用条件として特定のネットワークからのみ利用可と設定し、前記暗号化手段は前記特定の端末クライアントのネットワークアドレスでのみ前記配信情報の復号を可能とする暗号鍵を用いて該配信情報を暗号化し、前記端末クライアントは、前記ネットワークアドレスを取得する手段を備えたことを特徴とする請求項１３又は１４記載の配信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は配信システムに係り、特に利用条件を設定して配布されるデータ及びソフトウェアを利用者に配信する配信システムに関する。

【０００２】

【従来の技術】データ及びソフトウェアを試供目的や購入金額に応じて、利用回数、利用時間、利用期限、複写禁止が設定されて、配布されることが一般的に行われるようになってきており、その配信システムの一例が特開平７-３２５７１３号公報（発明の名称：利用時間の制約付きソフトウェア実行方法）にて提案されている。

【０００３】この従来の配信システムは、図１０に示すように、提供ソフトウェア９０１と、キー情報保存部９０２と、実行監視プログラム９０３と、インストール／複写プログラム９０４から構成されており、まず、提供ソフトウェア９０１の利用可能時間と、満期日時と、提供ソフトウェア９０１がインストールされているハードウェアの個別識別情報と、提供ソフトウェア９０１を記憶している記憶領域の物理的位置情報とを、暗号化してキー情報保存部９０２に記憶保持する。

【０００４】実行監視プログラム９０３は、キー情報保存部９０２に暗号化されて保持されている情報を参照し、ソフトウェアの実行の正当性を確認し、また、提供ソフトウェア９０１の実行中は、利用可能時間の監視を行い、時間を超過した場合に提供ソフトウェア９０１の実行を終了させる。インストール／複写プログラム９０４は、提供ソフトウェア９０１を計算機にインストールしたり、他の計算機に複写される際に使用される。

【０００５】この従来システムでは、インストール／複写プログラム９０４を使用せずに、提供ソフトウェア９０１をインストールや複写しても、暗号化されたキー情報を正しく復号できず、提供ソフトウェア９０１を実行できないので、提供ソフトウェア９０１の無制限な利用や複写を制限することができる。

【０００６】また、他の従来の配信システムとして、有償情報とインストールプログラムと利用情報とに対して読み出しができないように読み出し制限を施して提供者システムから利用者システムに配布する配布手段と、配布された上記の有償情報とインストールプログラムと利用情報とに対して読み出し制限の解除を行う制限解除手段と、読み出し制限が解除された利用情報に基づいて有償情報の利用の可否を判定する判定手段と、判定手段が肯定の判定をしたときのみ、読み出し制限が解除されたインストールプログラムを起動させると共に、読み出し制限が解除された有償情報を読み出してインストールプログラムに基づいて有償情報のインストールに必要な処理を行うインストール手段と、インストール手段によるインストールが終了した時に、読み出し制限が解除された状態の有償情報に読み出し制限を施して記憶手段に書き込む制限手段とを備えた配信システムも知られている（特開２０００-２００２２９：発明の名称「有償情報配布システム及び有償情報配布方法」。

【０００７】

【発明が解決しようとする課題】しかるに、上記の特開平７-３２５７１３号公報記載の従来システムの第１の問題点は、ソフトウェアの提供者は提供ソフトウェア９０１に対してプログラムの改造を必要とし、利用者配布の際には専用のインストール／複写プログラム９０４を必要とするということである。

【０００８】その理由は、正しい利用条件情報がなければ提供ソフトウェア９０１を停止するようなプログラムを付加する必要があるためである。また、専用のインストール／複写プログラム９０４を使用しないと、前記利用条件情報が正しくインストールされないためである。

【０００９】第２の問題点は、提供ソフトウェア９０１は暗号化されておらず、その改造が容易であるため、提供ソフトウェア９０１の違法な利用や複写が容易であるということである。

【００１０】また、上記の特開２０００-２００２２９記載の従来システムでは、利用制約付きの各種情報を利用者システムに配信し、配信先の利用者システムにおいてインストールが終了すると有償情報に読み出し制限を施して記憶手段に書き込むようにしているが、インストールプログラムの読み出し制限を行っていないため、他のプログラムによりインストールプログラムの解析が可能になってしまうという問題がある。また、利用条件を提供者システム側で管理することができないので、利用条件の変更が容易ではない。

【００１１】本発明は以上の点に鑑みなされたもので、利用制約付きのデータ及びソフトウェアを容易に作成し、利用者に配布し、かつ利用者が容易にそのデータ及びソフトウェアを利用できる利用制約付きソフトウェアの配信システムを提供することを目的とする。

【００１２】また、本発明の他の目的は、利用制約付きのデータ及びソフトウェアの違法な利用や複写を困難とする利用制約付きソフトウェアの配信システムを提供することにある。

【００１３】

【課題を解決するための手段】本発明は上記の目的を達成するため、利用制約付きデータ及びソフトウェアの少なくとも一方からなる配信情報を暗号パッケージ化して配信する配信サーバと、配信された利用制約付きデータ又はソフトウェアを利用する端末クライアントからなる配信システムであって、配信サーバは、利用制約付きデータ及びソフトウェアの少なくとも一方からなる配信情報の利用条件を管理及び設定する第１の管理手段と、配信情報と利用条件を、配信先の端末クライアントに対応する暗号鍵を用いて暗号化する暗号化手段と、配信先の端末クライアントに対応したプログラムの起動コードと暗号化された配信情報のインストール情報を管理及び設定する第２の管理手段と、暗号化された配信情報と、利用条件と、インストール情報とを１つの実行形式のプログラムにパッケージ化するパッケージ手段とを備え、端末クライアントは、サーバから配信されたパッケージを少なくとも記憶し、その後にパッケージ中の利用条件が暗号化されて更新記憶される記憶手段と、記憶手段から読み出した情報から暗号化された利用条件を抽出して、予め割り当てられた暗号鍵を用いて復号し、その復号した利用条件に応じて利用の許可・不許可を判定する判定手段と、記憶手段に記憶されたパッケージが判定手段により利用の許可されたパッケージである時には、そのパッケージ中の暗号化された配信情報を復号する復号手段と、復号手段からのソフトウェアのインストール処理を行ってから閲覧・利用するプログラムに処理制御を切り替える手段とを備えた構成としたものである。

【００１４】この発明では、利用制約付きデータや利用制約付きソフトウェアなどの配信情報を再コンパイルすることなく、利用条件を付加した後暗号化して端末クライアントに配信し、利用条件に応じて配信情報を復号して利用することができる。

【００１５】また、上記の目的を達成するため、本発明は、上記の端末クライアントを、判定手段により配信情報の利用が不許可と判定されたとき、又は他の任意のプログラムが起動されたときには、復号手段により復号された配信情報をアンインストールする手段を有することを特徴とする。

【００１６】この発明では、他の任意のプログラムが起動されたときには、復号手段により復号された配信情報をアンインストールすることができる。また、この発明では、端末クライアントにおいて、配信情報の利用時以外は暗号化された状態で保存しておくことができる。

【００１７】また、上記の目的を達成するため、本発明は、端末クライアントは、配信情報の利用開始時に実行情報を配信サーバに送信する送信手段と、配信情報の利用終了時に実行情報を配信サーバより取得して、復号された状態の配信情報を記憶領域より消去する手段を備えたことを特徴とする。この発明では、配信情報の利用開始時に利用条件などの実行情報を配信サーバに送信しているので、端末クライアントの利用条件などを配信サーバ側で管理することができる。

【００１８】

【発明の実施の形態】次に、本発明の実施の形態について図面と共に説明する。図１は本発明になる配信システムの第１の実施の形態のブロック図を示す。同図に示すように、本発明の第１の実施の形態は、利用制約付きの提供データ及びソフトウェアを暗号パッケージ化して配信する配信サーバ１と、配信されたデータ及びソフトウェアを利用する端末クライアント２から構成される。

【００１９】配信サーバ１は、端末クライアント２と通信する通信部１０と、提供データ及びソフトウェアを暗号化する暗号処理部１１と、暗号処理部１１が暗号処理する際に用いる暗号鍵を保持する暗号鍵管理部１２と、端末クライアント２に配信されたデータを実行するため

の起動情報を管理する起動情報管理部１３と、提供データ及びソフトウェアの利用条件を保持する利用条件情報管理部１４と、前記の起動情報と利用条件と暗号化された提供データ及びソフトウェアとをパッケージ化するパッケージ部１５と、提供データ及びソフトウェアの元データを保持する提供ソフトウェア保持部１６とを含む。

【００２０】端末クライアント２は、配信サーバ１と通信する通信部２０と、配信されたデータを復号化及び記憶領域上のデータを暗号化する暗号処理部２１と、暗号処理部２１が暗号処理する際に用いる暗号鍵を保持する暗号鍵管理部２２と、プログラムの実行状況を監視し、また、ある実行状況に対して割り込み処理を行う実行監視部２３と、実行監視部２３で用いられる各種情報を管理する実行情報管理部２４と、プログラムを実行処理するソフトウェア実行部２５とを含む。

【００２１】次に、図２のフローチャートを参照して図１の第１の実施の形態の配信サーバ１の動作について詳細に説明する。まず、配信サーバ１を起動すると、通信部１０において、端末クライアント２からの配信要求を待つ（ステップ１０１）。配信要求があると、暗号処理部１１は、要求された提供データ及びソフトウェアを提供ソフトウェア保持部１６より取得し（ステップ１０２）、その提供データ及びソフトウェアの暗号化に用いる暗号化アルゴリズムを選択する（ステップ１０３）。

【００２２】次に、暗号処理部１１は、配信要求に含まれている端末クライアント２固有の識別ＩＤに基づいて、配信要求元の端末クライアント２を識別し、暗号鍵管理部１２から、予め記憶されている配信先の端末クライアント２に対応した暗号鍵を抽出し（ステップ１０４）、抽出した暗号鍵と暗号アルゴリズムを用いて、提供データ及びソフトウェアを暗号化する（ステップ１０５）。

【００２３】次に、パッケージ部１５は端末クライアント２に配信される利用制約付きデータ及びソフトウェア（すなわち、提供データ及びソフトウェア）の起動情報を起動情報管理部１３より抽出する（ステップ１０６）。起動情報には、端末クライアント２に対応したプログラム起動コード、提供データ及びソフトウェアを端末クライアント２の記憶領域にインストールするインストールコード、提供ソフトウェアに制御が自動的に移るように設定されたプログラム終了コードを含む。上記のプログラム終了コードは、もし提供ソフトウェアが、画像データやテキストデータであれば、そのデータの形式に対応した閲覧ソフトウェアに制御が自動的に移るように設定されたプログラム終了コードとなる。

【００２４】次に、パッケージ部１５は端末クライアント２における提供データ及びソフトウェアの利用条件情報を利用条件情報管理部１４から抽出する（ステップ１０７）。利用条件情報には、利用回数、利用時間、利用期間、複写利用の可否、利用位置、利用者、利用端末、提供ソフトウェアの暗号化に使われた暗号アルゴリズムに関するパラメータのいずれかが含まれる。さらに、抽出した利用条件情報は、暗号処理部１１により暗号化される（ステップ１０８）。

【００２５】次に、パッケージ部１５は、ステップ１０５で暗号化された提供データ及びソフトウェア、ステップ１０６で生成された起動情報、ステップ１０８で暗号化された利用条件情報をパッケージ化する（ステップ１０９）。パッケージ化されたデータは、そのまま端末クライアント２で実行できる形式の配布実行パッケージとなる。暗号化された利用条件情報及び提供ソフトウェアは、配布実行パッケージのプログラムリソースとして扱われるように設定される。

【００２６】続いて、例えばパッケージ部１５が上記のステップ１０１ないしステップ１０９の一連の処理でエラーが発生したかどうかチェックし（ステップ１１０）、エラーがなければ、通信部１０はパッケージ部１５からの配布実行パッケージを端末クライアント２に配信し（ステップ１１１）、もしエラーがあれば、エラー情報を端末クライアント２に通知する（ステップ１１２）。

【００２７】次に、図３及び図４のフローチャートを参照して、図１の第１の実施の形態の端末クライアント２における配布実行パッケージを起動したときの動作について詳細に説明する。

【００２８】まず、端末クライアント２は通信部２０において、配信サーバ１より配信された配布実行パッケージを取得し、記憶領域に保存しておく。ソフトウェア実行部２５は、上記の記憶領域に保存されている配布実行パッケージを、利用者の指示で起動する（ステップ２０１）。実行監視部２３は、任意のプログラムの起動を監視しており、起動されたプログラムが配布実行パッケージかどうかを判断して、配布実行パッケージであれば、図４に示すフローチャートの処理を割り込み処理する（ステップ２０２）。

【００２９】割り込み処理では、実行監視部２３は、まず割り込み元の配布実行パッケージの識別情報を実行情報管理部２４に通知し、記録する（ステップ２１１）。さらに、暗号処理部２１は暗号鍵管理部２２より暗号鍵を抽出する（ステップ２１２）。暗号鍵管理部２２は、必要であれば、利用者のパスワード、端末の固有識別情報、端末のネットワークアドレス情報、地理的な位置情報を取得して、暗号鍵を生成する。

【００３０】続いて、暗号処理部２１は、抽出した暗号鍵を使って、まず利用条件情報を復号し（ステップ２１３）、更に、その復号された利用条件を参照して、提供データ及びソフトウェアの利用許可があるかどうかをチェックする（ステップ２１４）。利用実績回数が利用可能回数を上回ってないかどうか（残存利用回数がゼロより大きいかどうか）、利用実績時間が利用可能時間を上

回っていないかどうか（残存利用時間がゼロより大きいかどうか）、日時が利用期限を過ぎていないかどうか、複写されたデータかどうか、というチェックを必要であれば行う。複写されたデータかどうかは、例えば、利用条件に含まれたデータ操作日時と、端末クライアント２のファイルシステムによるデータ操作日時が一致しているかどうかで判断することが可能である。

【００３１】ステップ２１４において、提供データ及びソフトウェアの利用許可があると判断されたときには、暗号処理部２１は、提供データ及びソフトウェアの復号処理を行う（ステップ２１５）。他方、ステップ２１４において、提供データ及びソフトウェアの利用許可がないと判断された場合や、復号処理にエラーがあれば、実行情報管理部２４にその旨を通知し、記録する（ステップ２１６）。そして、割り込み元の配布実行パッケージに制御を戻す。

【００３２】割り込み処理終了後、実行情報管理部２４にエラーが通知されているがどうかをチェックし（ステップ２０３）、エラーがあれば、利用者にエラーの内容を通知する（ステップ２０５）。例えば、利用回数が規定回数以上になった、利用時間が規定時間以上になった、利用期限が過ぎた、データが複写など改竄されている、などのメッセージを図示しない表示部で表示する。表示後、実行情報管理部２４のエラーをクリアする。

【００３３】ステップ２０３において、実行情報管理部２４にエラーが通知されていないと判定されたときには、復号された提供データ及びソフトウェアを適切な記憶領域に記録し、インストール処理を行う（ステップ２０４）。次に、必要であれば、利用時間制限を設定するためにアラームタイマを登録する（ステップ２０６）。この時、登録されるアラームタイマのタイマ値は、利用条件を参照して、残り利用可能時間を抽出し、その残り利用可能時間に設定される。

【００３４】このタイマ値の時間を過ぎたら、配布実行パッケージをアラーム割り込み起動して実行を停止するように設定する。さらに、配布実行パッケージの処理を終了して、提供データの閲覧・利用ソフトウェアまたは提供ソフトウェアを起動して、処理制御を移す（ステップ２０７）。

【００３５】次に、図５及び図６の各フローチャートを参照して、図１の第１の実施の形態の端末クライアント２が、任意のプログラムを起動したときの動作について詳細に説明する。

【００３６】端末クライアント２は、ソフトウェア実行部２５で任意のプログラムを起動する（ステップ３０１）。実行監視部２３は、任意のプログラムの起動を監視しており、起動されたプログラムが配布実行パッケージの提供ソフトウェアかどうかを判断して、提供ソフトウェアでなければ、図６に示すフローチャートの処理を割り込み処理する（ステップ３０２）。

【００３７】割り込み処理では、まず、配布実行パッケージの識別情報を実行情報管理部２４より抽出する（ステップ３１１）。この配布実行パッケージの識別情報は、前記ステップ２１１で記録されたものであり、識別情報が存在してなければ、割り込み元のプログラムに制御を戻す。識別情報が存在していれば、提供データ及びソフトウェアを利用中ということになり、提供データ及びソフトウェアを他のプログラムによる複写や改竄を防ぐために、以下の処理を行う。

【００３８】また、割り込み元のプログラムの識別情報と一致している場合は、提供データ及びソフトウェアを利用しようとしているので、割り込み元のプログラムに制御を戻す。もし、提供データ及びソフトウェアが利用中であれば終了させる。

【００３９】実行情報管理部２４は、提供データ及びソフトウェアの利用した回数、時間などの利用履歴に関する利用条件情報を更新する（ステップ３１２）。次に、ステップ２１２と同様に、暗号処理部２１は、暗号鍵管理部２２より暗号鍵を抽出し（ステップ３１３）、抽出したその暗号鍵を使って、利用条件情報を暗号化する（ステップ３１４）。さらに、端末クライアント２の記憶領域に、配布実行パッケージから復号され、インストールされている提供データ及びソフトウェアを実行状態情報を含めて暗号化する（ステップ３１５）。提供データ及びソフトウェアは実行状態情報が存在しない、もしくは保存しておく必要がなければ、ステップ３１５の処理は省略してよい。

【００４０】次に、暗号化された利用条件情報、暗号化された提供データ及びソフトウェアを配布実行パッケージに格納する（ステップ３１６）。さらに、端末クライアント２にインストールされている提供データ及びソフトウェアを、アンインストールして、端末クライアント２の記憶領域から削除する（ステップ３１７）。必要であれば、メモリ領域もクリアする。

【００４１】もし、前記ステップ２０６において、アラームタイマが設定されていれば、これを解除する（ステップ３１８）。そして、割り込み元のプログラムに制御を戻す。割り込み処理終了後は、通常処理を行う（ステップ３０３）。

【００４２】このようにして、任意のプログラムを起動した時には、配布実行パッケージの識別情報が存在しているかどうか監視し、存在していなければ、提供データ及びソフトウェアの起動ではなく、他のプログラムの起動であるので、割り込み処理にてそれまで使用していた利用制約付きデータ及びソフトウェアを端末クライアント２の記憶領域から削除するようにしているため、利用制約付きデータ及びソフトウェアが、他のプログラムにより複写されたり改竄されてしまうことを防ぐことができる。ただし、利用制約付きデータ及びソフトウェアは暗号化して再びパッケージに格納しておく。

【００４３】次に、図７及び図８の各フローチャートを参照して、図１の第１の実施の形態の端末クライアント２が提供データ及びソフトウェアを利用中の動作について詳細に説明する。

【００４４】まず、前記ステップ２０６において設定されたアラームタイマによりアラーム通知がされると（ステップ４０１）、残存利用時間がゼロということで、提供データ及びソフトウェアの利用を終了し（ステップ４０２）、図６のフローチャートに示されたステップ３１２乃至ステップ３１８の処理を行う（ステップ４０３）。これにより、利用者はこれ以上提供データ及びソフトウェアを利用できない。

【００４５】また、実行監視部２３は、提供ソフトウェア実行中に、指定されたイベント処理を監視しており、指定されたイベント処理が発生すると（ステップ５０１）、図８のステップ５０２以降の割り込み処理を行う。指定されたイベント処理とは、ウィンドウの描画、利用者のマウスクリックなどのことである。

【００４６】割り込み処理においては、そのイベントが実行情報管理部２４に保持されている利用条件情報に登録されたイベントと一致するかどうかを調べる（ステップ５０２）。一致していなければ、通常処理に戻る（ステップ５０７）。一致していれば、利用履歴に関する利用条件情報を更新した後（ステップ５０３）、利用条件を参照して、まだ提供データ及びソフトウェアが利用可能かどうかをチェックする（ステップ５０４）。

【００４７】まだ利用可能であれば、通常処理に戻る（ステップ５０７）。利用不可であれば、提供データ及びソフトウェアの利用を終了し（ステップ５０５）、図６のフローチャートに示されたステップ３１２乃至ステップ３１８のアンインストール処理を行う（ステップ５０６）。

【００４８】次に、本実施の形態の効果について説明する。本実施の形態では、提供データ及びソフトウェアを再コンパイルすることなく、利用条件を付加及び暗号化を施し、端末クライアント２において実行可能な形式で配信するように構成されているため、利用制約付きのデータ及びソフトウェアを容易に作成し、利用者に配布し、かつ、利用者が容易に利用制約付きのデータ及びソフトウェアを利用することができる。

【００４９】また、本実施の形態では、さらに、端末クライアント２において、提供データ及びソフトウェアは利用時以外は暗号化された状態で保存されるように構成されているため、利用制約付きのソフトウェアの違法な利用や複写を困難とすることができる。

【００５０】次に、本発明の第２の実施の形態について図面を参照して詳細に説明する。図９は本発明になる配信システムの第２の実施の形態のブロック図を示す。同図中、図１と同一構成部分には同一符号を付し、その説明を省略する。図９に示すように、本発明の第２の実施の形態は、端末クライアント３が図１の第１の実施の形態における端末クライアント２に含まれている実行情報管理部２４を省いた構成となっている点に特徴がある。

【００５１】本実施の形態では、端末クライアント３は前記実行情報管理部２４に相当する情報管理機能を通信部２０を介して、配信サーバ側にデータを送信し、配信サーバ１の利用条件情報管理部１４で実行させるものである。必要であれば、通信時のデータの不正取得を防ぐために、配信サーバ１の暗号処理部１１と、端末クライアント３の暗号処理部２１を用いてデータを暗号化して通信することが可能である。暗号化通信の詳細は、従来より一般的に知られているので、本発明での説明は省く。

【００５２】次に、本実施の形態の効果について説明する。本実施の形態では、利用条件情報及び利用状況を配信サーバ１側で管理するように構成されているため、利用条件の不正な更新や改竄をより困難とすることができる。

【００５３】また、利用者が提供データ及びソフトウェアの利用料金を支払うなどによって、利用条件が更新された際でも、利用者の端末クライアント３に保持されているソフトウェアを更新することなしに、提供データ及びソフトウェアの利用条件を変更することができる。

【００５４】なお、本発明は以上の実施の形態に限定されるものではなく、例えば、第１及び第２の実施の形態では、配信サーバ１と端末クライアント２はインターネットなどの通信網を介してデータのやり取りを行うように構成されているが、フロッピー（登録商標）ディスク、ＣＤ-ＲＯＭなどの記録媒体を介してデータをやり取りするシステムにも本発明を適用できることは勿論である。

【００５５】また、通信網を介してデータのやり取りを行う場合でも、配信サーバ１が利用条件として特定のネットワークからのみ利用可と設定し、暗号処理部１１が特定の端末クライアントのネットワークアドレスでのみ利用制約付きデータ及びソフトウェアの復号を可能とする暗号鍵を用いて暗号化する構成とし、端末クライアント２又は３は、ネットワークアドレスを取得する構成としてもよい。更に、利用制約付きデータ及びソフトウェアの両方の配信に限らず、利用制約付きデータ及び利用制約付きソフトウェアの一方だけの配信でもよい。

【００５６】

【発明の効果】以上説明したように、本発明によれば、利用制約付きデータや利用制約付きソフトウェアなどの配信情報を再コンパイルすることなく、利用条件を付加した後暗号化して端末クライアントに配信し、利用条件に応じて配信情報を復号して利用するようにしたため、利用制約付きのデータ及びソフトウェアを容易に作成し、利用者に配布し、かつ利用者が容易にそのソフトウェアを実行できる配信システムを構築することができ

る。

【００５７】また、本発明によれば、他の任意のプログラムが起動されたときには、復号手段により復号された配信情報をアンインストールするようにしたため、他のプログラムにより復号された配信情報のデータの改竄やソフトウェアの解析や改竄などを防止することができる。

【００５８】また、本発明によれば、端末クライアントにおいて、配信情報の利用時以外は暗号化された状態で配信情報を保存しておくようにしたため、配信情報の違法な利用や複写を困難にすることができる。

【００５９】また、本発明によれば、配信情報の利用開始時に利用条件などの実行情報を配信サーバに送信することにより、端末クライアントの利用条件などを配信サーバ側で管理するようにしたため、利用条件の変更が容易にできる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態の構成を示すブロック図である。

【図２】第１の実施の形態の配信サーバの動作を示すフローチャートである。

【図３】第１の実施の形態の端末クライアントの提供データ及びソフトウェア利用時処理動作を示すフローチャートである。

【図４】第１の実施の形態の端末クライアントの提供データ及びソフトウェア利用時の割り込み処理動作を示すフローチャートである。

【図５】第１の実施の形態の端末クライアントの任意のソフトウェア実行時処理動作を示すフローチャートである。

【図６】第１の実施の形態の端末クライアントの任意のソフトウェア実行時の割り込み処理動作を示すフローチャートである。

【図７】第１の実施の形態の端末クライアントの提供ソフトウェア利用中のアラーム処理動作を示すフローチャートである。

【図８】第１の実施の形態の端末クライアントの提供ソフトウェア利用中のイベント割り込み処理動作を示すフローチャートである。

【図９】本発明の第２の実施の形態の構成を示すブロック図である。

【図１０】従来の一例のブロック図である。

【符号の説明】

１　配信サーバ

２、３　端末クライアント

１０、２０　通信部

１１、２１　暗号処理部

１２、２２　暗号鍵管理部

１３　起動情報管理部

１４　利用条件情報管理部

１５　パッケージ部

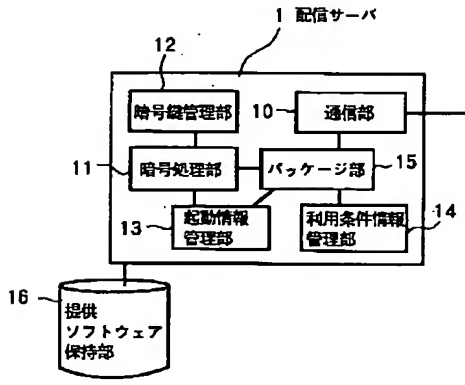
１６　提供ソフトウェア保持部

２３　実行監視部

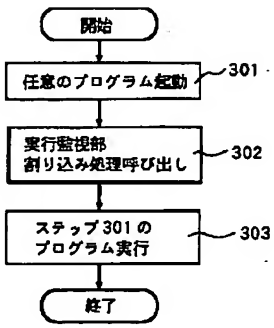
２４　実行情報管理部

２５　ソフトウェア実行部

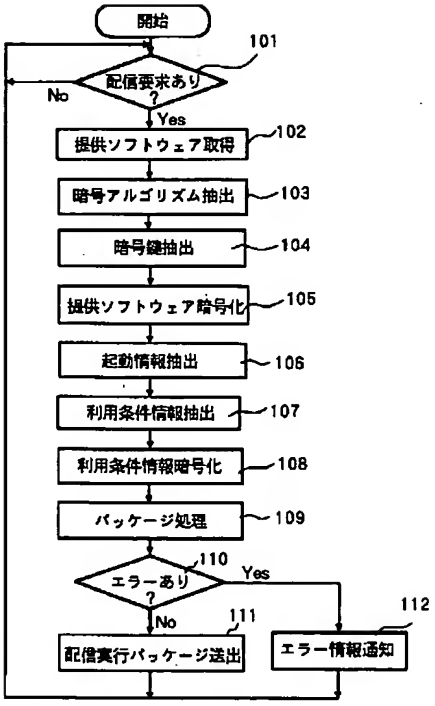
【図１】



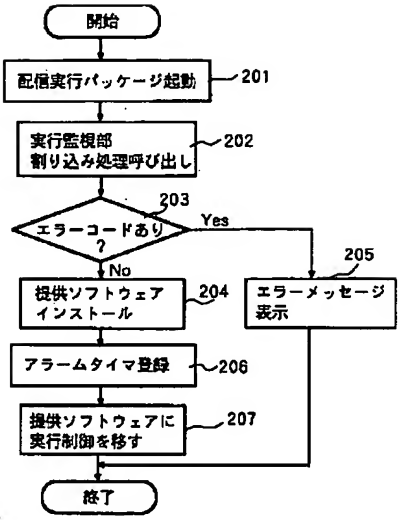
【図５】



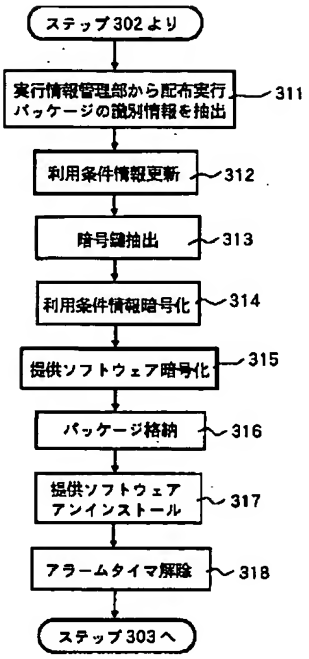
【図２】



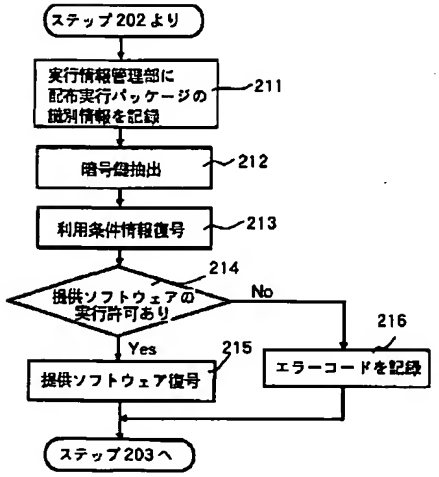
【図３】



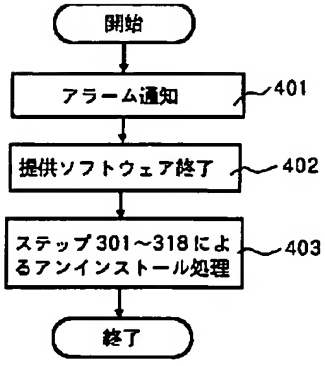
【図６】



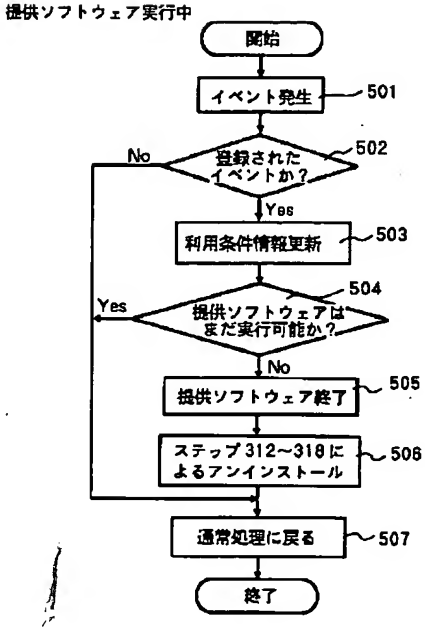
【図４】



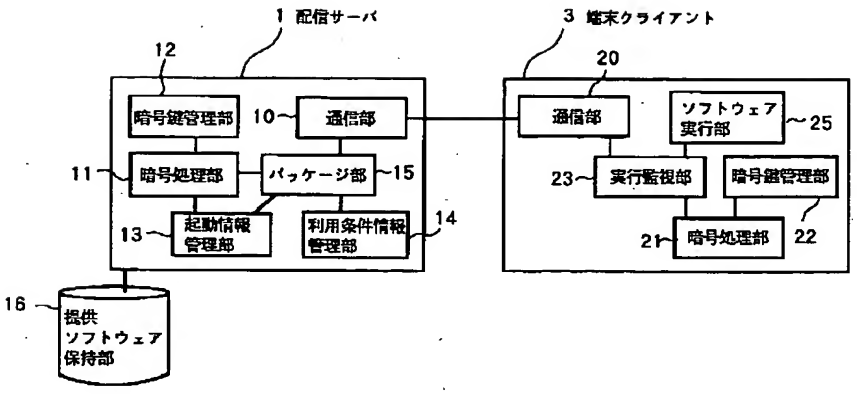
【図７】



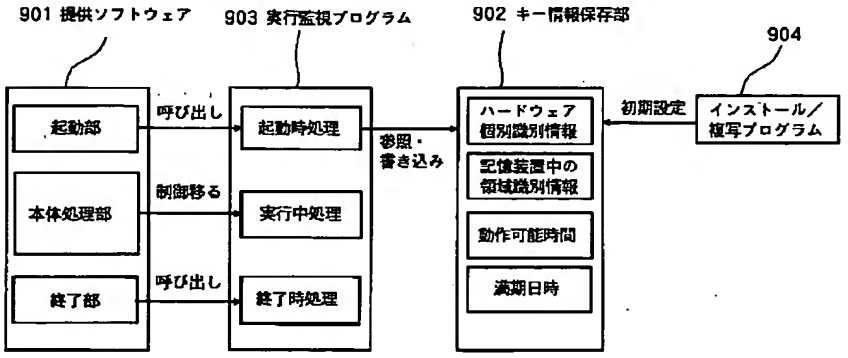
【図８】



【図９】


1 配信サーバ
3 端末クライアント
12
20
暗号鍵管理部
10
通信部
通信部
ソフトウェア実行部
25
11
暗号処理部
パッケージ部
15
23
実行監視部
暗号鍵管理部
13
起動情報管理部
利用条件情報管理部
14
21
暗号処理部
22
16
提供ソフトウェア保持部

【図１０】


901 提供ソフトウェア
903 実行監視プログラム
902 キー情報保存部
904
起動部
呼び出し
起動時処理
参照・書き込み
ハードウェア個別識別情報
初期設定
インストール／複写プログラム
本体処理部
制御移る
実行中処理
記憶装置中の領域識別情報
動作可能時間
終了部
呼び出し
終了時処理
満期日時